UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/623,037	08/24/2000	Michael Gundlach	P00.1249	5597

7590 07/08/2004

Kevin R. Spivak
Morrison & Foerster LLP
2000 Pennsylvania Avenue, N.W.
Washington,, DC 20006-1888

EXAMINER	
ZAND, KAMBIZ	
ART UNIT	**PAPER NUMBER**
2132	9

DATE MAILED: 07/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/623,037	GUNDLACH ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 August 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 August 2000* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *3/ 08-24-2000*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. **Claims 1-3** have been examined.

2. Foreign Priority benefit claimed under Title 35, United States Code, § 119 have been acknowledged.

3. The pages of PCT/DE98/02949 (paper number 2) have been considered.

4. Notice regarding power of attorney and the address change (paper number 7 and 8) has been acknowledged.

Drawings

5. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference sign(s) not mentioned in the description: Example: "FV-DEVICE" in fig. 1. Correction of all similar errors is requested.

6. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: Example " (MFV)" page 7, line 26 with respect to fig.1; "random number" page 8, line 14 with respect to fig.3 and -TIME'- page 8, line 13 with respect to fig.2; etc.; Correction of all similar errors is requested.

As an example, there is no "random number" in fig.3 but the description of figure 2 and 3 on page 8, lines 9-20 relates the "random number" to both figures. As another

example line 21-22 of page 8 describes "rpPIN" is generated by way of one-way function f and f'. However in fig.2, rpPIN is generated based on the inputs TIME, random # and PIN in contrast with fig.3 where rpPIN is generated by having output of one way function f which is the result of inputs TIME and PIN only and no random number as fig.1, as one input in addition with the second input TIME'. Therefore Examiner suggests the description of fig.2 and 3 be presented separately of each other where the definition of TIME', TIME and random number be in harmony with the figures 2 and 3 in clear language.

Specification

7. The abstract of the disclosure is objected to because of a typo error. Examiner considers the phrase "is" in line 8 as a typo error. Examiner suggests phrase "it" as a correct phrase in harmony with abstract language. Correction is required.

8. The disclosure is objected to because of the following informalities: Typo and grammatical errors. Examiner suggests the following corrections as examples:

- deletion of phrase "what are" from the phrase "These what are value-added services...incoming sources" in line 13 of page 1.
- deletion of phrase "the" from the phrase "...the this service, so.." in line 27 of page 1.

- The phrase "MFV" (pages 5-7) has to be written out for clarity. Applicant has referred to "MFV" as "multi frequency" only. Examiner suggests a clear description of the phrase that also includes the description of "V" within the phrase "MFV".

9. The specification has not been checked to the extend necessary to determine the presence of all possible minor errors. Applicant's cooperation is requested in correcting any errors of which applicant may become aware in the specification.
- Examiner suggests a new corrected specification pages (a clear copy and a markup copy) to be enclosed with the Applicants response to this office action.

10. Applicant is reminded of the duty to fully disclose information under 37 CFR 1.56.

Appropriate correction/clarification is requested.

Information Disclosure Statement PTO-1449

11. The Information Disclosure Statement submitted by applicant on 08/24/2000 (paper number 3) has been considered. Please see attached PTO-1449.

Claim Objections

12. **Claims 1-3** are objected to because of the following informalities: typo error. Examiner suggests the following corrections:

Claim 2:

- Delete "a" (line 4, first occurrence) from the phrase " variable parameter is **a** selected from the group...".
- Replacement of "the" (line 4) with "a" in the phrase " variable parameter is a selected from **the** group..".

Claim 3:

- Replacement of phrase "the" (line 4) with "a" in the phrase " encoding function is selected from **the** group..".

- **Claim 1** is objected to because of the following informalities: The phrase "unambiguous digit sequence" (line 5) is confusing. Examiner suggests deletion or replacement of phrase "unambiguous" from the phrase since an unambiguous digit number to one may be an ambiguous digit number to another. It is Examiner understanding that Applicant uses the "unambiguous digit number" to refer to a unique input digit number such as PIN for the purpose of examination. Appropriate clarification or correction is requested.

Claim Rejections - 35 USC § 112

13. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

14. **Claim 2** is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

In claim 2, the "can be.." phrase (line 6) makes the claims indefinite and unclear in that neither method steps nor interrelationship of method steps are set forth in these claims in order to achieve the desired results expressed in the "can be..." phrase.

It is not clear "can be" is an affirmative statement with respect to claim 1 or not and whether Examiner should consider that the method steps are being executed (narrow claim language) or not (broader claim language).

In claim 2, the phrase " a number taken from a number sequence that can be calculated" is confusing since it is not clear if Applicant implies that the number sequence consist of also numbers that are not functional numbers for encoding numbers in the light of claim 1 encoding process or consist of non-digit variable parameters or not. It is also confusing if this sequence number is considered as any pick numbers from a number sequence in addition of PIN and TIME and "Random Number" or it is related to the PIN, Time or Random Number selection. Examiner

considers " a number taken from a number sequence that can be calculated" as a variable parameter that corresponds to a PIN for the purpose of examination in harmony with figure 2 and 3. Clarification or correction is requested.

Claim Rejections - 35 USC § 102

15. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

16. **Claims 1 and 2** are rejected under 35 U.S.C. 102(e) as being anticipated by Elliot et al. (5,867,495 A).

As per claim 1 Elliott et al (5, 867, 495 A) teach a method for securing access of a user to a service in an intelligent telecommunication network (**see fig.1c; 10a; 19a-b,e; col.6, lines 39-49; col.11, lines 59-67; col.12, lines 1-62 where services and accesses features are described and col.39, lines 26-32 where data access is restricted and authenticated by encryption as one option and therefore it is a secure access of a user to services available to the user**), comprising the steps of: entering, by said user, an unambiguous digit sequence in a terminal device, said digit sequence being only known to said user of said service (**see col.39, lines 26-32 disclose the storage of sequence pins such as password or PINs and secure transmission of those if needed; fig.42 and col. 58, line 34-35 disclose user enters userid and passcode and col.60, line 57-59 disclose the passcode is only known to the user**); encoding said digit sequence and additional variable parameter using encoding function which thus produces a function calculating result containing said digital sequence (**col.132, lines 63-67; col.133, lines 1-14 where a digit sequence such as user PIN, a variable parameter such as pseudo-randomly generated number of six digit that changes every 60 seconds are encoded with RSA and DES encryption key, that is the encoding function which produce a calculating result for authentication**), using multi-frequency dial method in said communication network up to a central entity (**see fig.19a, item 1 and 10 with respect to item 2 and fig.17-18; col.66, lines 39-40; col.124, lines 27-34 where DTMF is described as multi frequency method; and fig. 19a disclose item 1 and 10 communicate with central entity and col.132, line 49 disclose dial-in method**); and evaluating said

transmitted digit sequence in said central entity and permitting said user to use said service if said evaluation is positive (**see col.133, lines 7-15 where after verification of the transmitted result and user's pin and the access code, if verified the access to resources granted**) and if a previously transmitted said digit sequence has not been received within a fixed time interval (**see col.132, lines 63-67; col.133, lines 1-14 a variable parameter such as pseudo-randomly generated number of six digit that changes every 60 seconds, therefore the time interval is only 60 seconds for login or another sequence number that is being generated has to be transmitted**).

As per claim 2 Elliott et al (5, 867, 495 A) teach a method according to claim 1, wherein said variable parameter is selected from a group consisting of a time specification, a random number, and a number taken from a number sequence that can be calculated (**see col.132, lines 63-67; col.133, lines 1-14 where a variable parameter selected as a pseudo-randomly generated number of six digit that changes every 60 seconds**)

Claim Rejections - 35 USC § 103

17. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

18. **Claim 3** is rejected under 35 U.S.C. 103(a) as being unpatentable over Elliott et al (5, 867, 495 A) in view of Bruce Schneier (Applied cryptography; second edition; Katherine Schowalter/ John Eiley & Sons, Inc. 1996; pages 29, section 2.3 and 30; page 576, authentication protocol –page 577 up to but not including section 24.1).

As per claim 3 Elliott et al (5, 867, 495 A) teach all limitation of the claim but do not disclose said encoding function is selected from the group consisting of a single-step method according to ITU X.509, a two-step method according to ITU X.509, a method according to RFC 1938, and a hash function. However Bruce Schneier disclose encoding method according to one-way function where the function takes a variable length input string and converts it to fixed length output string (see pages 29, section 2.3 and page 30). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Bruce Schneier's one way function disclosure in Elliot et al's encryption scheme using a six digit random number and a passcode in order to produce an encoding function that works one way and therefore a collision free function that is extremely difficult to be compromised during the communication of the user or caller and the central entity.

Bruce Schneier also disclose X.509, a two-step method according to ITU X.509 (**see page 576, authentication protocol –page 577 up to but not including section 24.10; where in a single step X.509 it establishes trust between Alice and Bob by establishing their identities and the integrity of any communication between them; and in two step method adds a reply from Bob the receiver**). It would have

been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Bruce Schneier's

X.509 one step or two step encoding function disclosure in order to prevents any reply attack on the communication when utilizing X.509 one step and also establishing secrecy of both communication and reply attack when utilizing X.509 two-step method.

19. **Claim 3** is rejected under 35 U.S.C. 103(a) as being unpatentable over Elliott et al (5, 867, 495 A) in view of Haller et al. (one-time password system, RFC 1938; May 1996; Network Working Group; pages 1-17).

As per claim 3 Elliott et al (5, 867, 495 A) teach all limitation of the claim but do not disclose said encoding function method according to RFC 1938. However Haller et al disclose RFC 1938 encoding method where generation of one-time password is being done by combining all inputs and a computation step where the secure hash function is applied a specific number of times (**see page 3 of 17, section 6**). It would have been obvious tom one of ordinary skilled in the art at the time the invention was made to utilize RFC 1938 encoding method in Elliot et al's encryption scheme in order to prevent user's secret passcode to be transmitted cross the network at any time such as during the authentication of the user or caller.

Conclusion

20. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

a. U.S.Patent No. US (6,125,457 A) teach networked computer security system.

b. U.S.Patent No. US (5,995,624 A) teach bilateral authentication and information encryption token system and method.

c. U.S.Patent No. US (5,892,828 A) teach user presence verification with single password across applications.

d. U.S.Patent No. US (6,061,799 A) teach removable media for password-based authentication in a distributed system.

e. U.S.Patent No. US (5,351,295 A) teach secure method of neighbor discovery over a multi-access medium.

f. U.S.Patent No. US (5,060,263) teach computer access control system and method.

g. U.S.Patent No. US (4,800,590) teach computer key and computer lock system.

h. U.S.Patent No. US (4,652,698) teach method and system for providing system security in a remote terminal environment.

i. U.S.Patent No. US (6,064,736 A) teach systems, methods and computer program product that use an encrypted session for additional password verification.

j. U.S.Patent No. US (5,825,884 A) teach method and apparatus for operating transactional server in a proprietary database environment.

k. U.S.Patent No. US (5,944,824 A) teach system and method for single sign-on to a plurality of network elements.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (703) 306-4169. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

06/25/04

AU 2132